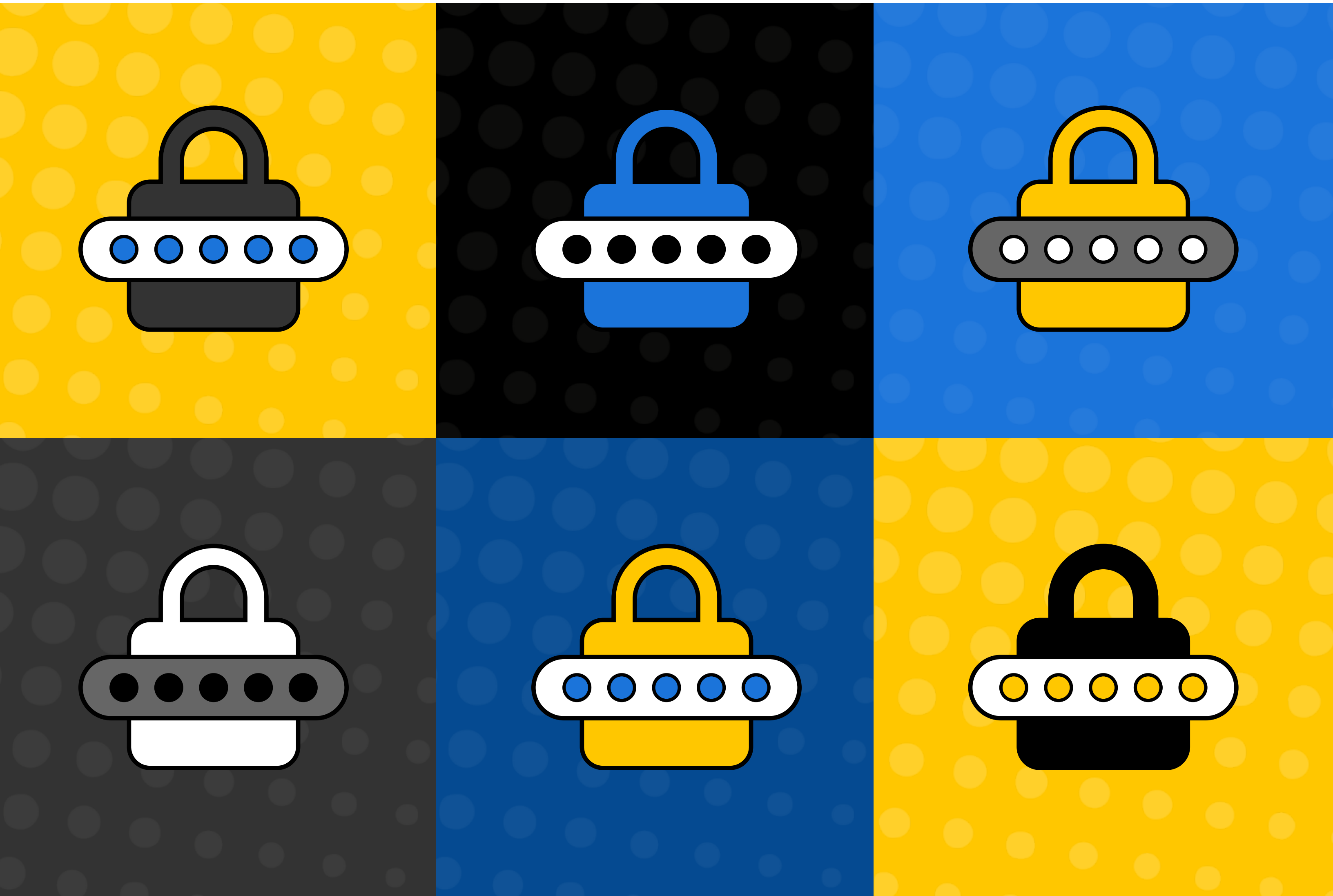
KEEPER
Cybersecurity Starts Here®

2022
UK PASSWORD PRACTICES REPORT



FOREWORD

Online passwords are used for critical aspects of our lives. They are needed when we communicate, work, transact and travel. We use them to access our most sensitive data, from our banking to health records. Digital passwords are the keys to our lives.

Yet we are surprisingly negligent about password protection; including our choice of passwords, the means we use to remember them, and troublingly, our willingness to share sensitive passwords with others.

Our survey of 4,000+ respondents in the UK and the US unearthed negligent attitudes toward password protection, in which passwords are being shared with spouses, written down on bits of paper, changed too often and forgotten over 40 times per year!

The consequence: half of our 2,000 UK survey respondents had been hacked at least once, with £295 stolen per cyberattack. Yet 15% of respondents said they were happy to carry on a normal life despite being the victim of an attack.

The consequences of poor password protection can be disastrous in an era of growing online crime and identity theft. A hacked password can result in ransacked bank accounts, obliterated credit ratings, damaged personal lives and severed business relationships.

As we are more digitally dependent than ever, poor password protection only contributes to the growing threat of cyberattacks. The average adult in the UK has access to nine connected devices, with 85% of people using smartphones to go online. Consequently, the chances of a critical personal data breach are very real, particularly when there are over 2,000 cyberattacks a day.

To raise awareness of the scale of the problem of weak passwords, Keeper Security, the leading provider of zero-trust and zero-knowledge cybersecurity software, surveyed UK password practices essential to our cybersecurity.

By raising awareness of the personal finances and personal data put at risk every day by weak, duplicated and shared passwords, we hope to reduce cybercrime and promote better password practices.

EXECUTIVE SUMMARY

Our research was conducted by Censuswide, an independent market research consultancy, between the 11th and 15th of August 2022. The survey took place via an online link with 4,007 nationally representative respondents (18+) in the UK and US. Censuswide are members of the British Polling Council, abide by and employ members of the Market Research Society which is based on the ESOMAR principles.

Through this data, we found that:

Despite the growing awareness of hacking, the British public is ignoring basic password hygiene and unwittingly offering up information to cybercriminals and scammers, leading to breaches of personal information and loss of funds.

We found that over half of our 2,000 survey respondents had been hacked at least once, and on average, people in the UK had £295 stolen per cyberattack. A quarter (24%) of our respondents said their social media account logins were also stolen as a result of being hacked.

The report also analysed cybercrime across the UK, unearthing Cardiff, Birmingham, and Leeds as hacking hotspots, where people experienced cyber crime at a higher rate. In Cardiff, 23% of respondents have experienced some form of hacking, followed by Birmingham and Leeds (both 18%), compared to the UK average of 14.9%.

The report found a major cause of cyberattacks is a troublingly casual attitude to password protection. Nearly a quarter (24%) of respondents aged 25-34 have trusted their partner/spouse with their passwords, and 23% surveyed write their passwords down on a sticky note or in a journal. This flies in the face of the most basic security protocols in existence, when it is common knowledge never to write a password down or share it with others.

This casual attitude was also present when 15% of people surveyed said they were happy to carry on as normal, despite knowing they had been hacked.

Gauging the level of importance people attached to their passwords in the UK, we asked respondents what they would rather happen compared to losing all their passwords.

Over one in 10 said they would rather have a root canal treatment than lose their passwords! 23% said they would rather lose access to television. This demonstrates a concern for password protection and is indicative of the likelihood of passwords being duplicated. Our research found a nearly half (49%) of UK respondents use the same password for multiple sites or apps. We also found respondents use their birthdates as passwords, a dangerous cross-pollination of sensitive information.

Given the attitudes and behaviours on display in the study, it’s alarming that UK consumers are turning a blind eye to password hygiene. It demonstrates a pressing need for the public to adopt better cybersecurity by using a trusted password management system.

FINDINGS

Poor password management and the consequences

Protecting your password

Nearly one-quarter (24%) of respondents aged 25-34 have trusted their partner/spouse with their passwords, compared to under a fifth (18%) of respondents aged 55-64 who said the same.

The top five passwords respondents used were: 14% pet's name, 12% family member's name, 10% a family member's birthday, 10% mother's maiden name, 9% their own birthday.

One in seven respondents aged 18-24 use their birthday when creating passwords, compared to one in 16 respondents aged 55-64 who said the same, pointing to a more reckless attitude to cybercrime among the young.

These findings also point to the availability of easy-to-guess passwords by other family members or close associates.

Password duplication

Nearly half (49%) of respondents use the same password for multiple sites/apps, and on average, respondents use the same password for four different sites/apps.

A fifth (20%) of male respondents use the same password for six to ten different sites/apps, whereas 1 in 7 (14%) female respondents said the same.

As a result, the likelihood of having multiple accounts affected by a cyberattack is a real possibility in the UK.

49%

Of respondents reuse their passwords

14%

Use a pet's name in passwords

The impact of being hacked

Half of respondents in our poll have been the victim of a cyberattack at least once, with a fifth (20%) of respondents saying money was stolen as a result. On average, respondents lost £295.

Just under a quarter (24%) of respondents said their social media accounts' logins have been stolen, with an even higher percentage for those 18-24. Almost a third (32%) of respondents in that group have had their social media logins stolen as a result of a breach.

Meanwhile, 15% of the survey said they know their passwords are compromised or available on the dark web.

How much do we value our passwords?

Just over 1 in 6 respondents aged 25-34 would rather get a root canal than lose all their passwords.

Just under a quarter (24%) of respondents aged 25-34 would rather be stood up on a date than lose all their passwords.

Over 72% of respondents aged 65+ said, when thinking of passwords, security is most important to them, whilst just over half (51%) of respondents aged 18-24 said the same.

PEOPLE SAY LOSING ALL THEIR PASSWORDS IS WORSE THAN...

22% Being stood up on a date

23% Not watching TV for a week

12% Getting a root canal

MAINTAINING GOOD HYGIENE AND REDUCING PASSWORD OVERLOAD

Remembering and changing passwords

We found that on average, respondents forget their password 48 times a year.

Respondents aged 18-24 forget their password 61 times a year, compared to respondents aged 65+ who forget theirs 39 times a year.

On average, respondents in our study changed their password 11 times per year, and just over 1 in 8 (13%) respondents change their password once a month.

Remembering and changing passwords is clearly problematic and points to widespread security loopholes.

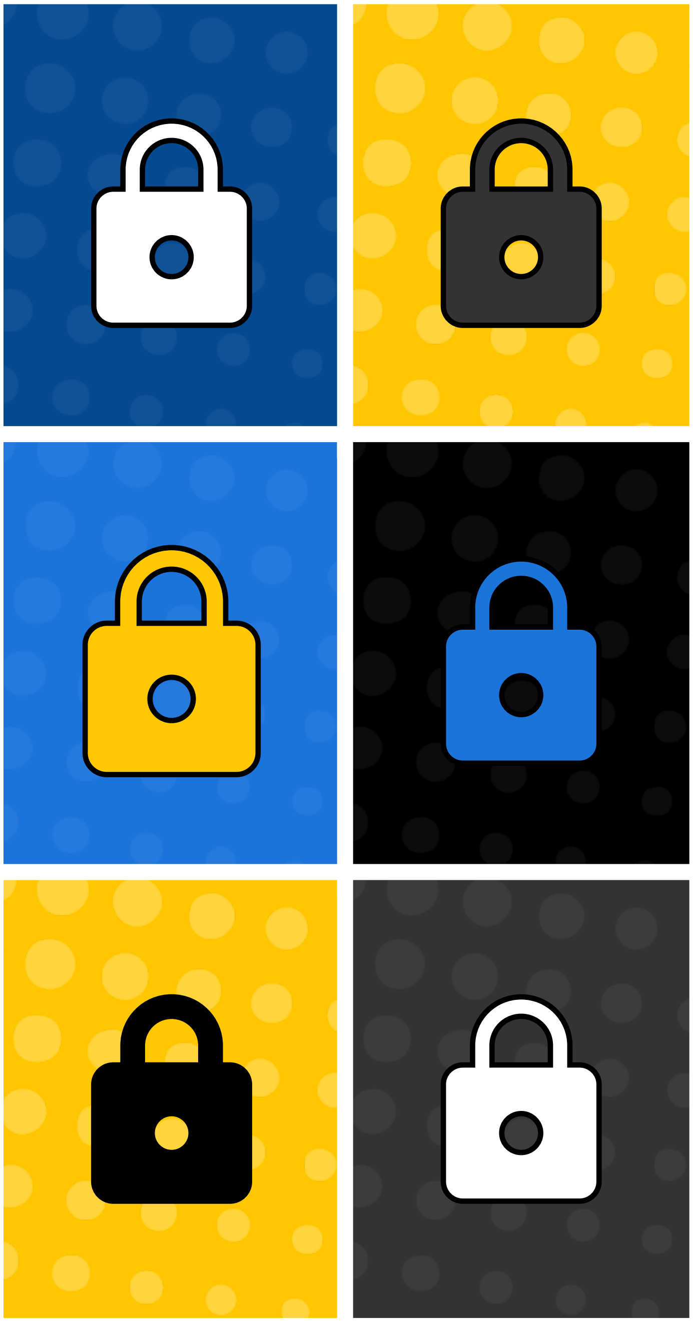
25% of the survey say they 'just remember' their passwords, but for the more forgetful among us, the results were troubling.

The most common method of remembering a password, particularly among older age groups, was physically writing it down: 23% said they kept their password on sticky notes, in a diary, or on a notepad. Nearly two in five of those over 65 kept passwords with this method. Among respondents aged 35-44, only 14% said the same. Further, 14% of respondents used password management software, yet 9% chose to store passwords in their web browsers.

These instances show that potential hackers have ready access to our most sensitive devices and data.

23%

said they kept their password on sticky notes, in a diary, or on a notepad



How many password-protected accounts/ apps do we have?

On average, respondents aged 18-24 report having 27 password-protected accounts/apps. Respondents aged 55-64 say they have 18. Male respondents have 25 password protected accounts/apps, whereas female respondents have 18.

There is, therefore, a pressing need for solid password protection across a number of devices.

Using password locks

Over half (52%) of respondents use a passcode to unlock their phone.

Just over 1 in 8 (13%) of respondents use a passcode to access their gaming device.

A third (33%) of respondents aged 65+ do not secure their phone with a passcode.

Using multi or two-factor authentication (MFA/2FA)

Almost a fifth of respondents have used 2FA but find it difficult to use.

Likewise, 18% of respondents have not used MFA because they're worried it is too difficult to use.

KNOW THE RISKS AND STAY VIGILANT

Spotting and identifying cyberattacks

Over 6 in 10 (63%) of respondents said they would be confident in identifying phishing emails.

Nearly three in five (57%) respondents were confident they could spot a phoney social media message coming from a friend who didn't send it.

Over half (53%) of respondents would be confident in identifying a message that could trigger a ransomware attack, however, just under a fifth (19%) would not.

Are we worried about being hacked?

Almost 7 in 10 (68%) respondents are concerned about what would happen if they were to be hacked, but just 3 in 10 (30%) were very concerned, pointing to a casual attitude towards the implications of a cyber breach.

Will I be the victim of a cyberattack?

Just under 29% of respondents think they are likely to be hacked, with just over 1 in 20 saying very likely. This tallies with a separate survey carried out in 31 countries around the world between October and November 2020, which revealed that a third of respondents thought at least one of their online accounts (e.g. email, social media, banking) would be hacked the following year.

63%

Of respondents are confident in identifying phishing emails

57%

Of respondents were confident they could spot a phoney social media message

53%

Of respondents would be confident in identifying a message that could trigger a ransomware attack

CONCLUSION

We have found a troubling disconnect between the value people attach to their passwords and the means they use to protect them. In the UK, people would rather see a dentist than lose their passwords, yet safe selection, storage, and management of passwords were found to be severely lacking in this study.

It was of great concern to see passwords being shared and duplicated across multiple platforms. Troubling also, to see the use of overly simple passwords, relying on data available elsewhere, such as names and birthdays. This will remain an acute challenge as we continue to use a range of devices and platforms to access the internet. The impact of poor password protection was evidenced by the number of people in the survey reporting being hacked, resulting in financial loss and compromised social media profiles.

The report showed, most of all, that cybersecurity relies on attitudes. Despite demonstrating a high awareness of cybercrime, we noted a reluctance to take action against it, ranging from forgoing multi-factor authentication to not responding to a cyber breach, despite knowing it had taken place. Yet, unchecked, cybercrime will only get worse.

Today cybercrime costs the UK economy £27 billion a year, the National Crime Agency reports. NCA also notes ‘a significant growth in cyber criminality in the form of high-profile ransomware campaigns over the last year. Breaches leaked personal data on a massive scale leaving victims vulnerable to fraud… cybercriminals seek to exploit human or security vulnerabilities to steal passwords, data or money directly.’ The most common cyber threats noted by the NCA include hacking - including of social media and email passwords, phishing emails, malicious software and distributed denial of service (DDoS) attacks against websites.

We all hold a responsibility to practise better internet hygiene as society becomes more interconnected. In 2021, it was estimated that 319.6 billion emails were sent and received daily around the world. Every one of these emails can be used to commit cybercrime, and conversely, every one of the emails will need to be sent by someone following sound cybersecurity protocols, which start with solid password protection and practices. Our survey found that there is a high likelihood that this protection will be rudimentary at best. It need not be this way. The tools and techniques exist for safer password creation and storage across multiple devices and now is the time to utilise them.

About Keeper Security

Keeper Security, Inc. (“Keeper”) is transforming the way organizations and individuals protect their credentials, secrets, connections and sensitive digital assets to significantly reduce the risks of identity security-related cyberattacks, while gaining visibility and control. Keeper is the leading provider of zero-trust and zero-knowledge security cloud services trusted by millions of people and thousands of organizations for password management, secrets management, privileged access, secure remote infrastructure access and encrypted messaging.

Keeper’s products are the highest-rated in the industry across G2, Trustpilot, PCMag and U.S. News & World Report. For the last several years, Keeper has received several InfoSec Awards from Cyber Defense Magazine for its cybersecurity enterprise software. Keeper is SOC 2 and ISO 27001 certified, FIPS 140-2 validated and FedRAMP Authorized. Keeper is backed by Insight Partners, a leading venture capital and private equity firm with $90b AUM.